

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
 «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**ОТЧЁТ**

**по лабораторной работе №10 «Настройка параметров мандатного управления доступом и мандатного контроля целостности»**

**по дисциплине «Защита в операционных системах»**

Выполнил: студент гр. ВКБ41

Якушевский С.С.

Проверил:

доц. Скляров А.В.

асс. Кацай А.М.

г. Ростов-на-Дону

2024 г.

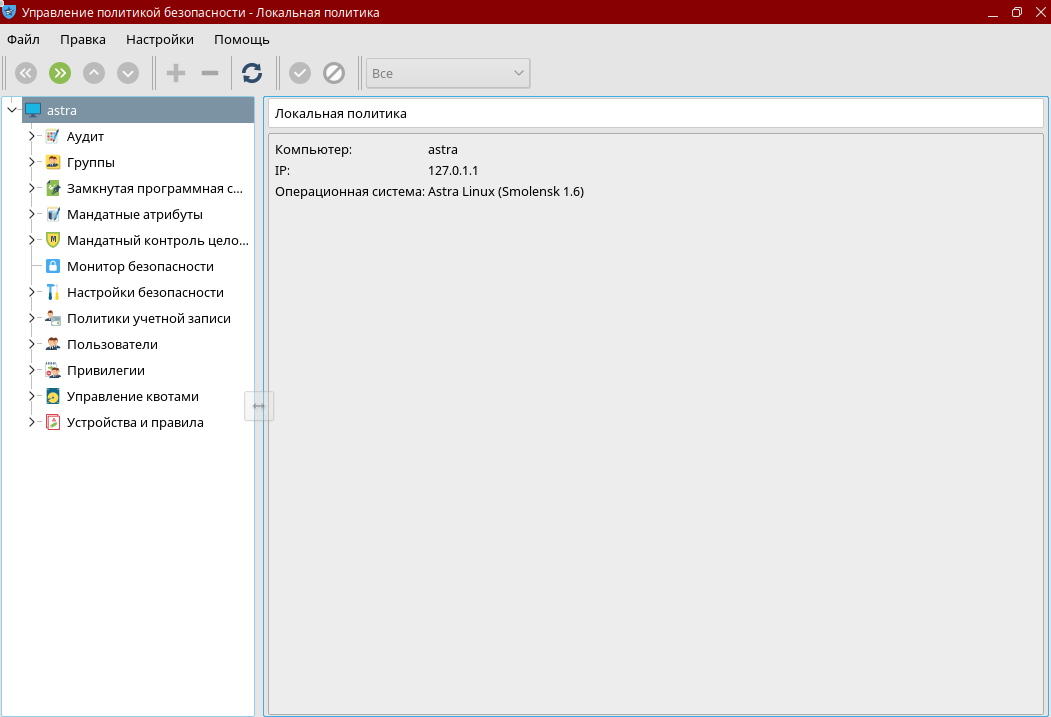
**Цель работы:** освоить администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд.

Ход работы:

1. Начать работу со входа в ОССН в графическом режиме с учётной записью с привилегированного пользователя (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).

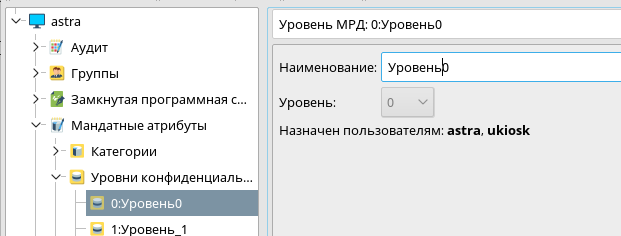


1. Запустить графическую утилиту редактирования учётных записей пользователей «Политика безопасности» через меню «Панель управления» главного пользовательского меню.

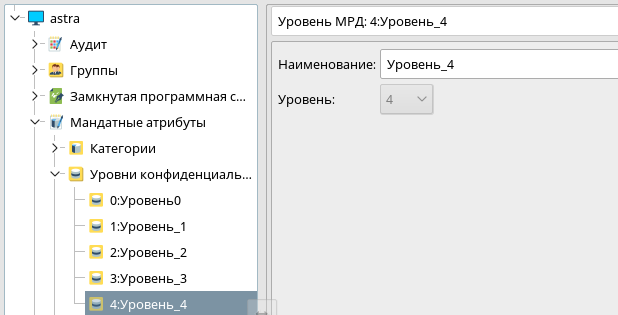


1. Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия:

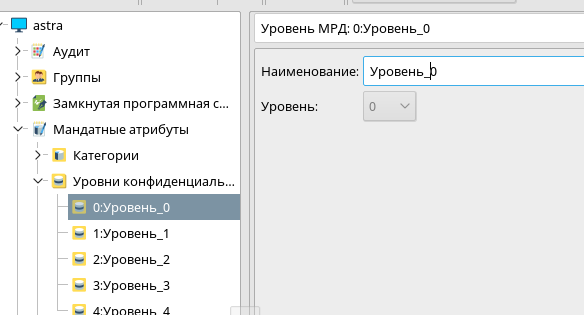
• открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать «0»: Уровень\_0» и переименовать данный уровень доступа: «Уровень0»;



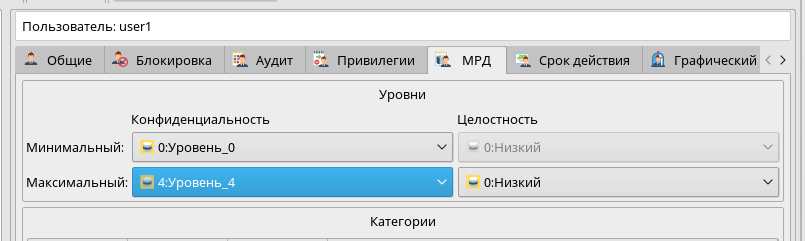
• выполнить создание уровня доступа с именем «Уровень \_4», задав значение равное 4, после чего проверить наличие записи «Уровень\_4» в списке «Уровни конфиденциальности»:



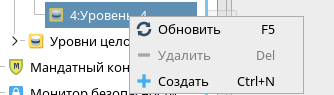
• выполнить обратное переименование: «Уровень0» в «Уровень \_0».



1. Создать учётную запись пользователя user1, установив максимальный уровень доступа: «Уровень\_4».



1. Попытаться удалить уровень доступа 4 из раздела «Уровни конфиденциальности» путём выбора в контекстном меню пункта «Удалить». Объяснить результат.

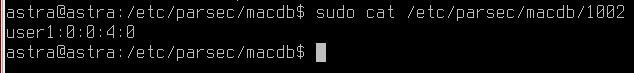


1. Вывести в терминал Fly параметры мандатного управления доступом для учётной записи пользователя user1. Для этого выполнить следующие действия:

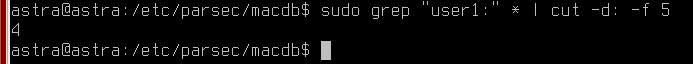
* запустить терминал Fly и перейти в каталог /etc/parsec/macdb;



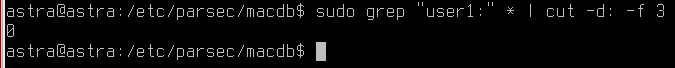
* прочитать параметры учётной записи user1 командой sudo cat /etc/parsec/macdb/XXXX (XXXX – UID пользователя user1).



* определить максимальный уровень доступа учётной записи user1 командой sudo grep "user1:" \* |cut -d: -f 5;

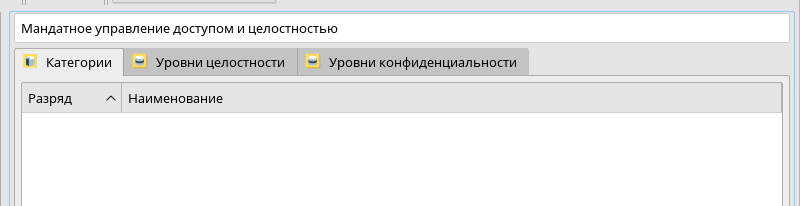


* определить минимальный уровень доступа учётной записи user1 командой sudo grep "user1" \* |cut -d: -f 3 и проверить его соответствие данным, отображаемым в графической утилите «Политика безопасности».

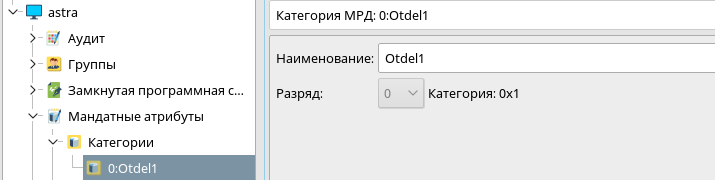


Создать неиерархические категории с использованием графической утилиты «Политика безопасности». Для этого выполнить следующие действия:

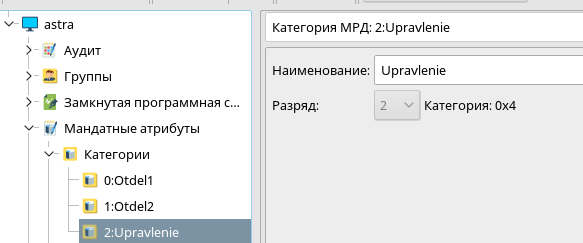
* в разделе «Категории» (Панель управления → Безопасность → Мандатные атрибуты → Категории) удалить исходные неиерархические категории;



* затем создать новую неиерархическую категорию с именем «Otdel1», «Разряд» - 0;

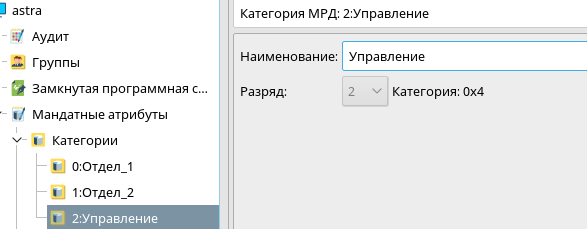


* в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2).



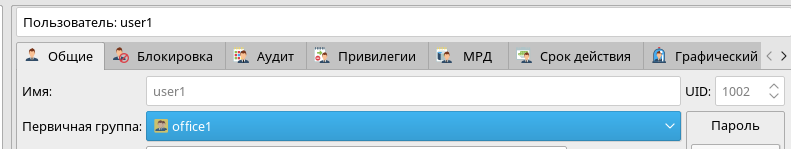
1. Изменить набор неиерархических категорий с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия в разделе «Категории»:

* выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел\_1»;
* аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел\_2» и «Управление», соответственно.

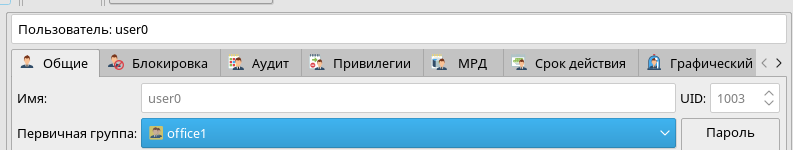


1. Изменить мандатный уровень доступа с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия:

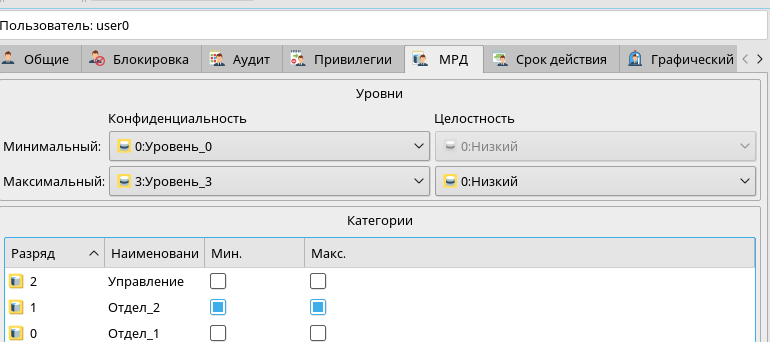
• создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 - «office1»;



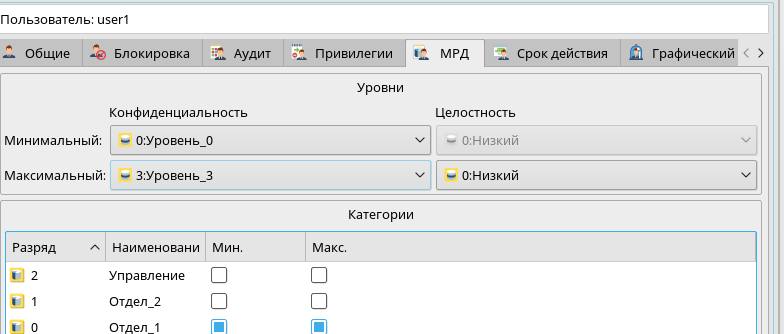
• создать новую учётную запись пользователя user0 и установить её первичную группу – «office1»;



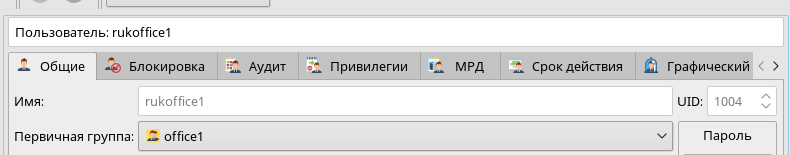
• для учётной записи пользователя **user0** в вкладке «МРД» выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2»;



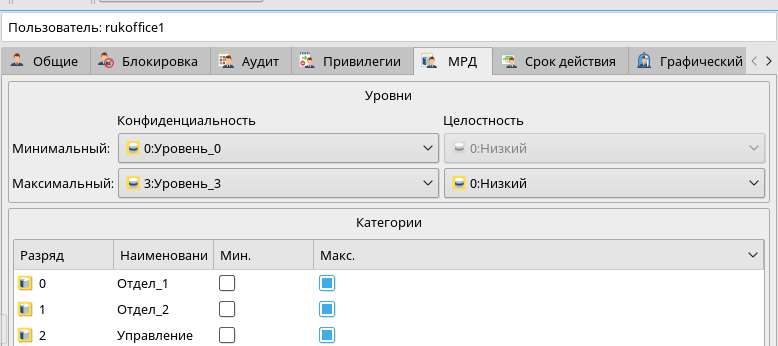
• Открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1»;



• создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1»:



• в вкладке «МРД» пользователя rukoffice1 выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление».



1. Создать общий каталог для работы от имени учётных записей пользователей user1, user2, rukoffice1 в каталоге /home/work. При этом, для работы от имени учётных записей пользователей с наборами неиерархическими категорий равными «Отдел\_1», «Отдел\_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «uрr» соответственно. При этом обеспечить хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия:

• запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;



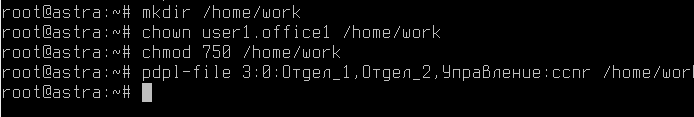
• создать каталог work и задать параметры мандатного и дискреционного управления доступом командами:

mkdir /home/work

chown user1.оffice1 /home/work

chmod 750 /home/work

pdpl-file 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work



• создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами:

cd /home/work

mkdir otdel1

chown user1:оffice1 otdel1

chmod 770 otdel1

pdpl-file 3:0:Отдел\_1:ccnr otdel1



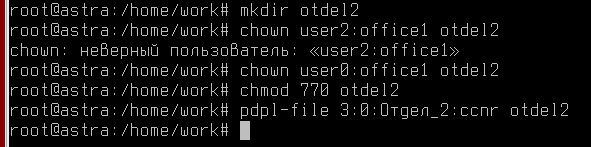
• создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел\_2» и задать параметры мандатного и дискреционного управления доступом командами:

mkdir otdel2

chown user2:office1 otdel2

chmod 770 otdel2

pdpl-file 3:0:Отдел\_2:ccnr otdel2



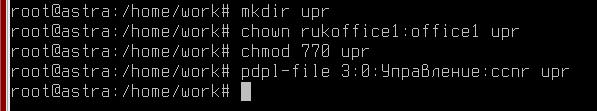
• создать каталог uрr для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Управление» командами:

mkdir uрr

chown rukoffice1:оffice1 uрr

chmod 770 uрr

pdpl-file 3:0:Управление:ccnr uрr



• создать вложенные каталоги Y1, Y2, YЗ в каталогах otdel1, otdel2, upr командами:

mkdir -p otdel1/{Y1,Y2,Y3}

mkdir -p otdel2/{Y1,Y2,Y3}

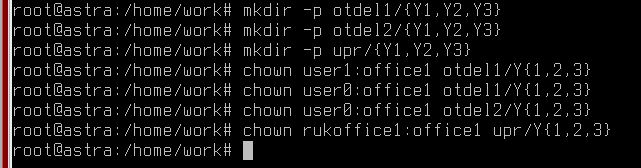
mkdir -p upr/{Y1,Y2,Y3}

и установить соответствующие владельца и группу владельца файлов:

chown user1:office1 otdel1/Y{1,2,3}

chown user2:office1 otdel2/Y{1,2,3}

chown rukoffice1:office1 upr/Y{1,2,3}



(user0 был назначен владельцем otdel1 по ошибке)

• установить для каталогов otdel1, otdel2, upr необходимые уровни (см. команды для каталога upr):

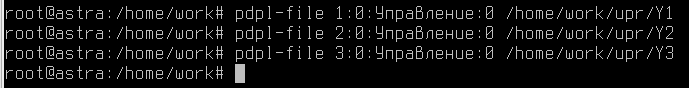
pdpl-file 1:0:Управление:0 /home/work/upr/Y1

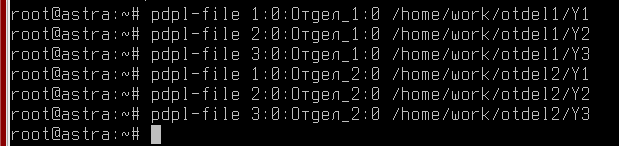
pdpl-file 2:0:Управление:0 /home/work/upr/Y2

pdpl-file 3:0:Управление:0 /home/work/upr/Y3

chown rukoffice1.office1 upr/Y{1,2,3}

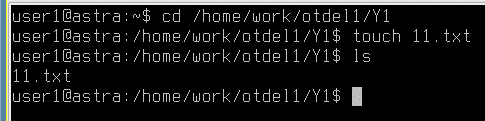
chmod 770 upr/Y{1,2,3}

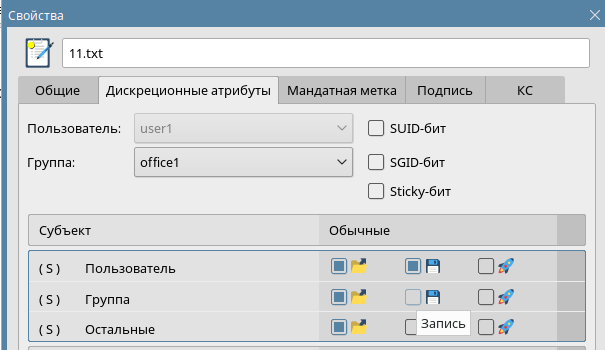




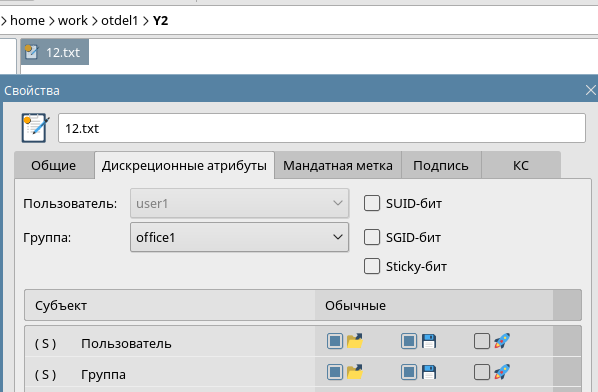
1. Выполнить последовательные входы в ОССН с учётной записью пользователя user1 (неиерархическая категория — «Отдел\_1», уровни доступа 1, 2, 3). При работе на уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel1/YX файлы с именами 11.txt, 12.txt, 13.txt соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы оffice1 в графическом файловом менеджере Fly (fly-fm).

Уровень 1:

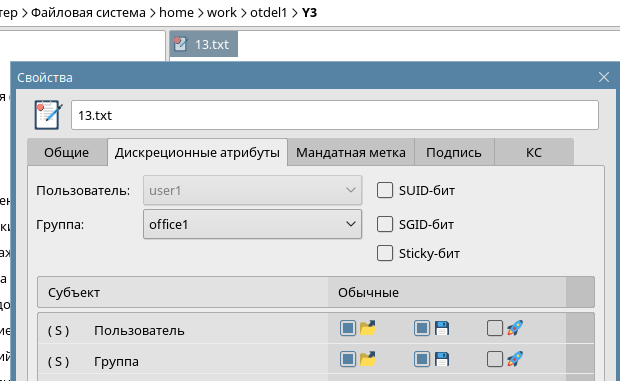




Уровень 2:

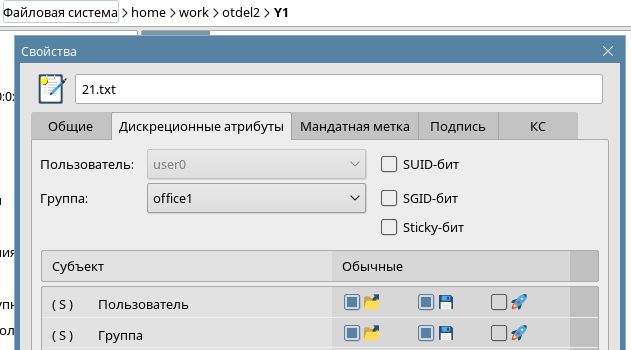


Уровень 3:

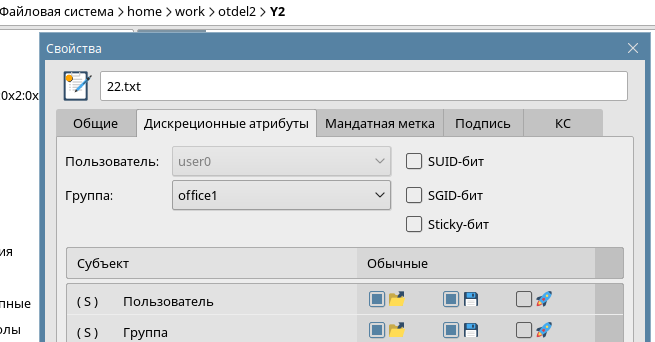


1. Выполнить последовательные входы в ОССН с учётной записью пользователя usег2 (неиерархическая категория — «Отдел\_2», уровни доступа 1, 2, 3). При работе на мандатных уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel2/YХ файлы с именами 21.txt, 22.txt, 23.txt соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы office1 в файловом менеджере Fly (fly-fm).

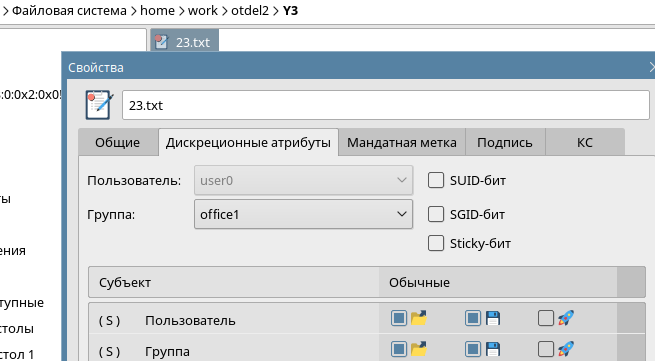
Уровень 1:



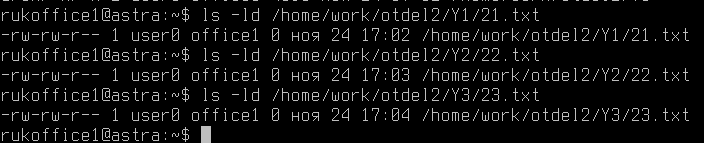
Уровень 2:



Уровень 3:

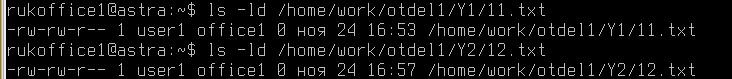


1. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа - 3, неиерархическая категория — «Отдел\_2») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 21.txt, 22.txt, 23.txt, доступ на запись к файлу 23.txt.



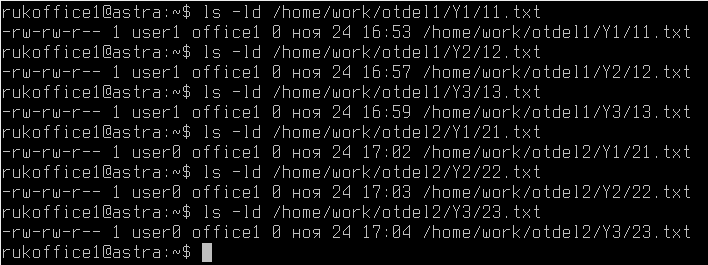
Есть доступ на чтение и запись к файлам 21.txt, 22.txt, 23.txt

1. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 2, неиерархическая категория — «Отдел\_1») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 11.txt, 12.txt, доступ на запись к файлу 12.txt.



Есть доступ и на чтение, и на запись.

1. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, набор неиерархических категорий — «Отдел\_1», «Отдел\_2», «Управление») и проверить возможность получения доступа на чтение к файлам 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.



Для всех шести файлов есть доступ на чтение.

1. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, неиерархическая категория — «Управление»). Создать файл u3.txt в каталоге /home/work/uрr/Y3.

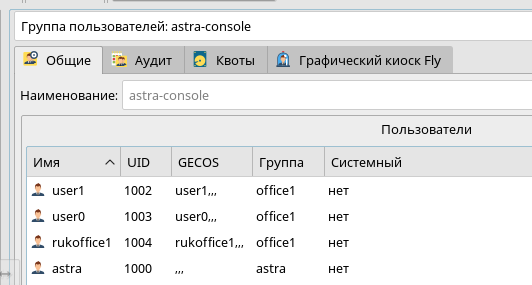


1. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, набор неиерархических категорий: «Отдел\_1», «Отдел\_2», «Управление») и проверить возможность получения следующих доступов к файлам: доступ на запись к файлу u3.txt, доступ на чтение к файлам u3.txt, 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt. Объяснить результат.



У всех вышеперечисленных файлов есть доступ и на чтение, и на запись.

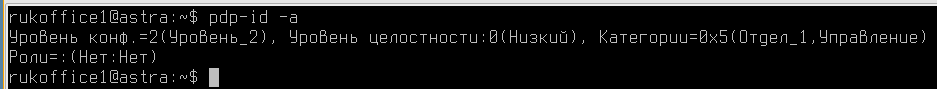
1. Для доступа к терминалу Fly настроить включение учётных записей пользователей user1, user2, rukoffice1 во вторичную группу astra-console. Это позволит данным учётным записям пользователей запускать терминал Fly с использованием комбинации Win+R.



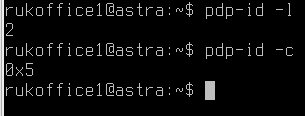
1. Вывести в терминал Fly параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей. Для этого выполнить следующие действия:

- войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 2, набор неиерархических категорий: «Отдел\_1», «Управление»);

- в терминале Fly выполнить команду pdp-id -а, проанализировать результат;



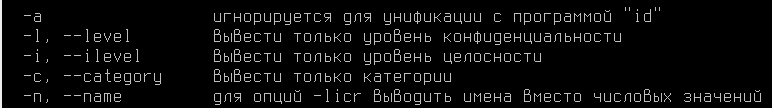
- выполнить избирательный вывод параметров мандатного управления доступом (с числовыми значениями) командами pdp-id -l и pdp-id -с;



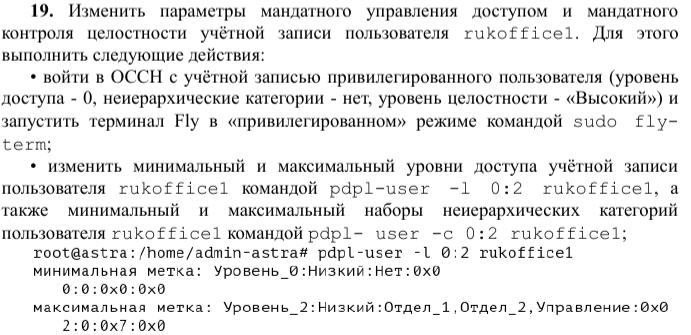
- выполнить избирательный вывод параметров мандатного управления доступом (с именами) командами pdp-id -ln и pdp-id -сn.

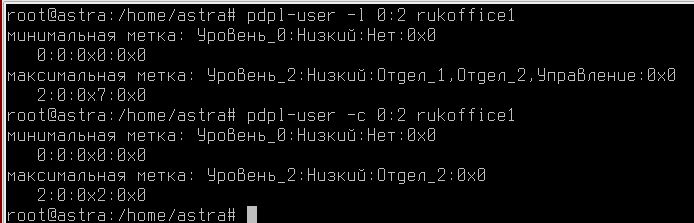


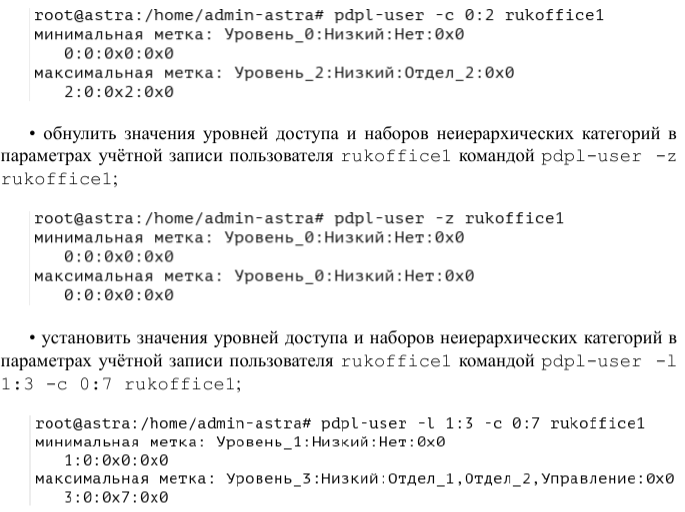


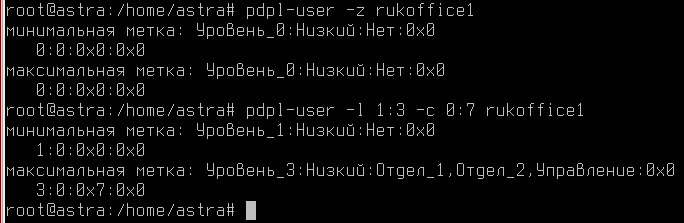


(буква n добавляет буквенный вывод)







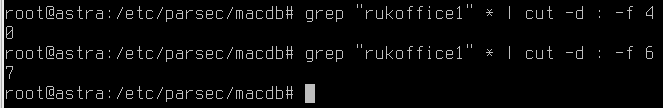


1. Считать параметры мандатного управления доступом и мандатного контроля целостности учётной записи пользователя rukoffice1 из файлов настроек. Для этого выполнить следующие действия:

• перейти в каталог /etc/parsec/macdb и считать минимальный и максимальный уровни доступа командами grep "rukoffice1" \* | cut -d : -f 3 и grep "rukoffice1" \* | cut -d : -f 5 соответственно;

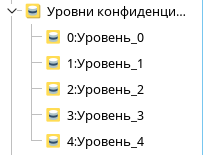
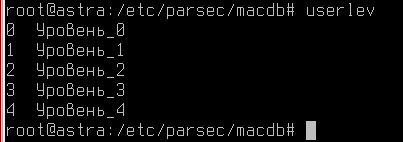


• считать минимальный и максимальный наборы неиерархических категорий командами grep "rukoffice1" \* | cut -d : -f 4 и grep "rukoffice1" \* | cut-d : -f 6 соответственно.

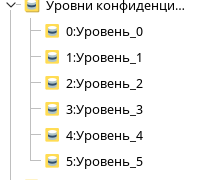
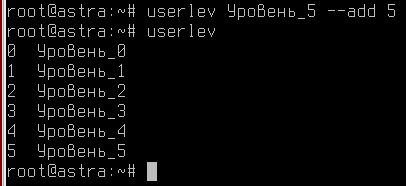


1. Создать и модифицировать мандатные уровни доступа, осуществив следующие действия:

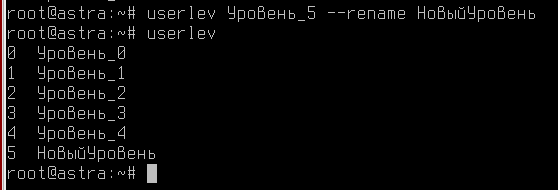
• вывести в терминал созданные уровни доступа командой userlev и сравнить полученные данные с настройками в утилите «Политика безопасности»;



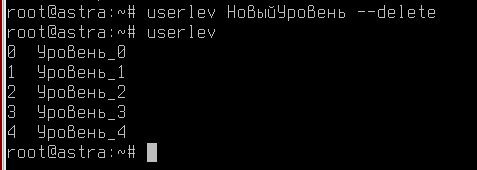
• добавить новый уровень доступа с именем «Уровень\_5» (значение 5) командой userlev Уровень\_5 --add 5 и вывести в терминал уровни доступакомандой userlev;



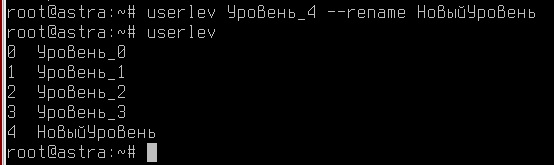
• выполнить переименование уровня доступа «Уровень\_5» в «НовыйУровень» командой userlev Уровень\_5 --rename НовыйУровень;



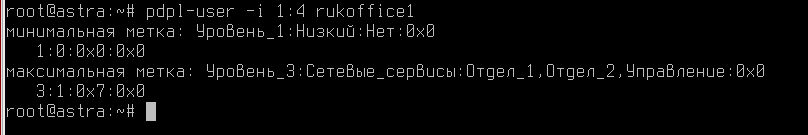
• удалить уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень --delete и вывести в терминал уровни доступа командой userlev.



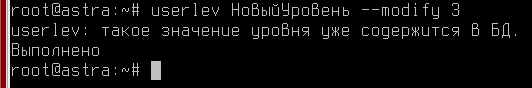
• выполнить переименование уровня доступа «Уровень\_4» в «НовыйУровень» командой userlev Уровень\_4 --rename НовыйУровень.



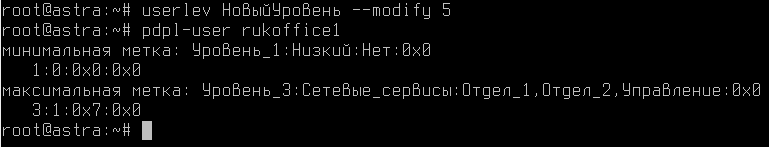
• добавить возможность работы от имени учётной записи пользователя rukoffice1 на уровне доступа 4 командой pdpl-user -i 1:4 rukoffice1;



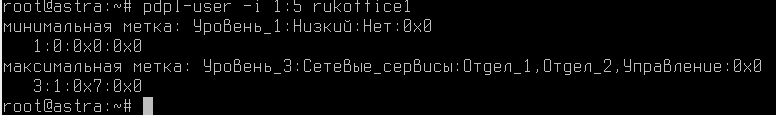
• выполнить попытку изменения значения уровня доступа «НовыйУровень» на 3 командой userlev НовыйУровень --modify 3, проанализировать результат;



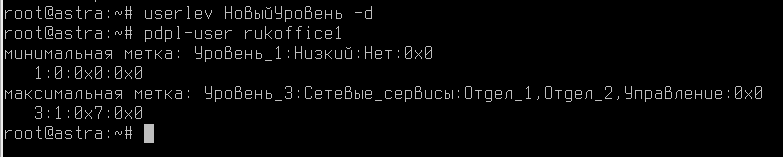
• изменить значение уровня доступа «НовыйУровень» на 5 командой userlev НовыйУровень --modify 5 и вывести в терминал максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1, проанализировать результат;



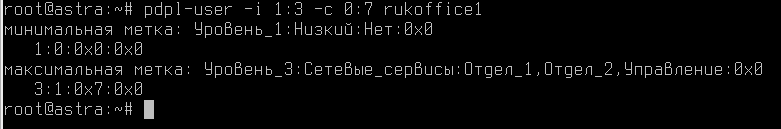
• установить максимальный уровень доступа учётной записи пользователя rukoffice1 равным 5 командой pdpl-user -i 1:5 rukoffice1;



• удалить уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень -d и определить максимальный уровень доступа учётной записи пользователя rukoffice1 командой pdpl-user rukoffice1, проанализировать результат;

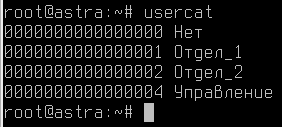


• восстановить набор неиерархических категорий и уровней доступа учётной записи пользователя rukoffice1 командой pdpl-user -i 1:3 -с 0:7 rukoffice1.



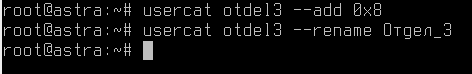
1. Создать и модифицировать неиерархические категории:

• в терминале Fly, запущенном в «привилегированном» режиме, вывести неиерархические категории командой usercat;

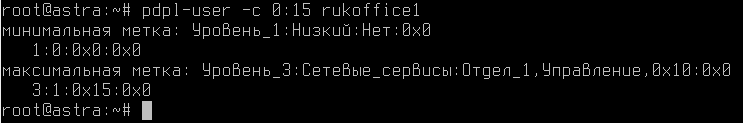


• добавить новую неиерархическую категорию командой usercat otdel3 --add 0x8;

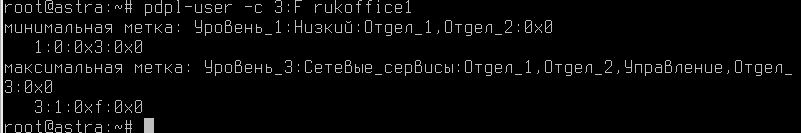
• переименовать неиерархическую категорию «otdel3» в «Отдел\_3» командой usercat otdel3 --rename Отдел\_3;



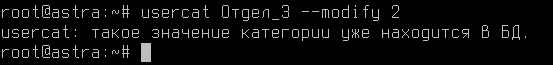
• осуществить попытку модификации наборов неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 0:15 rukoffice1, проанализировать результат;



• добавить неиерархическую категорию «Отдел\_3» в наборы неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user -с 3:F rukoffice1, обратить внимание на то, что неиерархическая категория задаётся в шестнадцатеричном формате;



• осуществить попытку изменения значения неиерархической категории «Отдел\_3» на значение 2 командой usercat Отдел\_3 --modify 2, проанализировать результат;



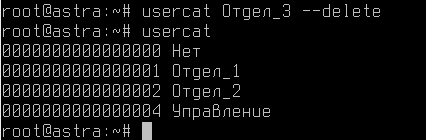
• изменить значение неиерархической категории «Отдел\_3» на 0x10 командой usercat Отдел\_3 --modify 10;



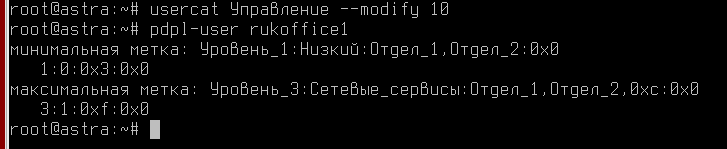
• изменить значение неиерархической категории «Отдел\_3» на 0x20 командой usercat Отдел\_3 --modify 0x20, обратить внимание на то, что независимо от указания типа числа по префиксу «0х» (десятичное или шестнадцатеричное) значение неиерархической категории задаётся в шестнадцатеричном формате;



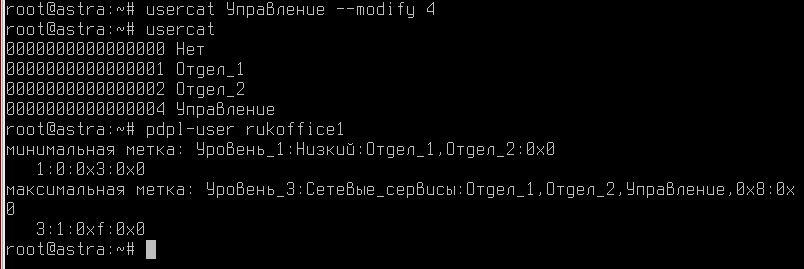
• удалить неиерархическую категорию «Отдел\_3» командой usercat Отдел\_3 --delete;



• изменить значение неиерархической категории «Управление» на 0x10 командой usercat Управление --modify 10, проанализировать результат по данным, выводимым командой pdpl-user rukoffice1;

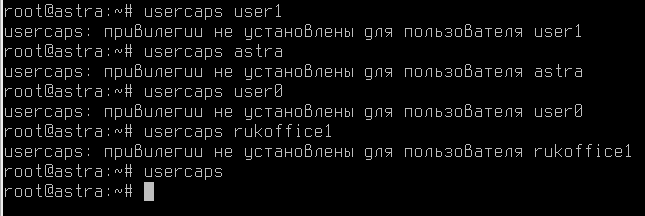


• изменить значение неиерархической категории «Управление» на 4 командой usercat Управление --modify 4

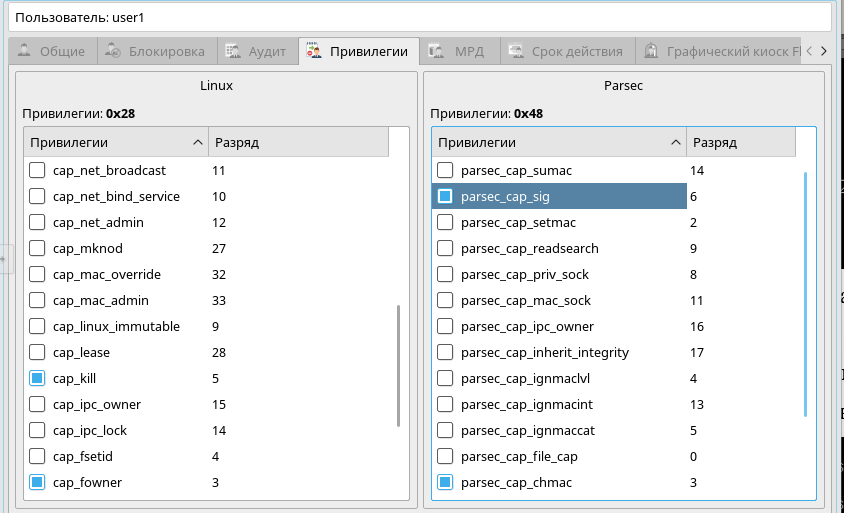


1. Для настройки привилегий учётных записей пользователей осуществить следующие действия:

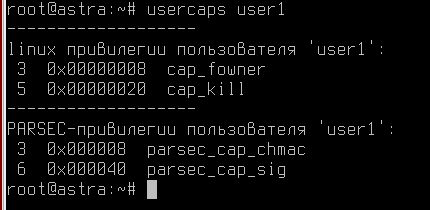
• вывести в терминал заданные в ОССН привилегии учётных записей пользователей командой usercaps, при работе в терминале Fly в «привилегированном» режиме;



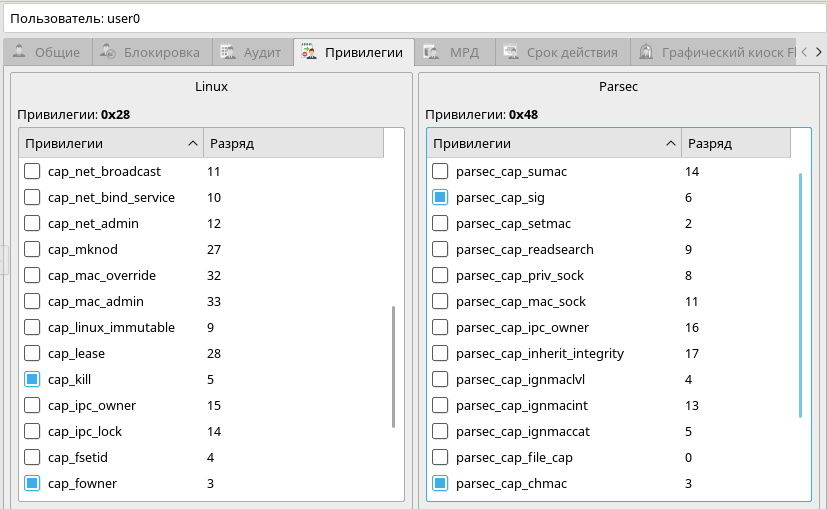
• запустить графическую утилиту «Политика безопасности» и открыть настройки учётной записи пользователя user1, в вкладке «Привилегии» установить Linux-привилегии cap\_kill, cap\_fowner и PARSЕС-привилегии parsec\_cap\_chmac, parsec\_cap\_sig, после чего закончить работу с утилитой



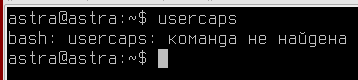
• вывести привилегии учётной записи пользователя user1 командой usercaps user1;



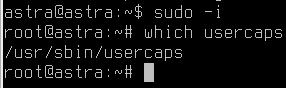
• в графической утилите «Политика безопасности» открыть параметры учётной записи пользователя user2, в вкладке «Привилегии» выбрать Linux-привилегии cap-kill, cap\_fowner и PARSEС-привилегии parsec\_cap\_chmac, parsec\_cap.sig,



• запустить терминал Fly в «непривилегированном» режиме командой fly-term и осуществить попытку запуска команды usercaps,



• определить расположение файла usercaps командой which usercaps, выполненной из «привилегированного» режима, а затем выполнить в «непривилегированном» режиме команду /usr/sbin/usercaps, проанализировать результат;

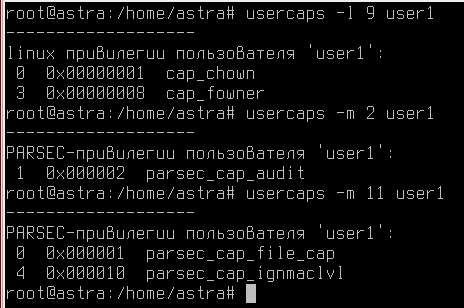




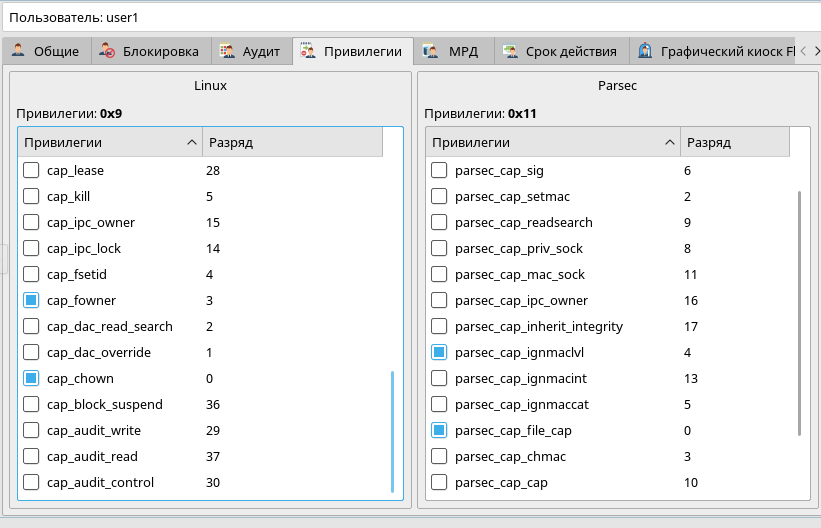
• запустить терминал Fly в «привилегированном» режиме командой sudo fly-term и выполнить модификацию Linux-привилегий и РАRSЕС-привилегий командами: usercaps -l 9 user1;

usercaps -m 2 user1;

usercaps -m 11 user1.

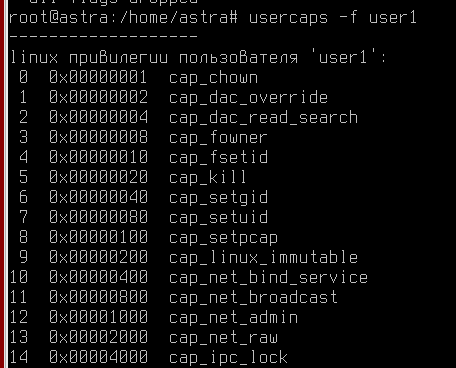
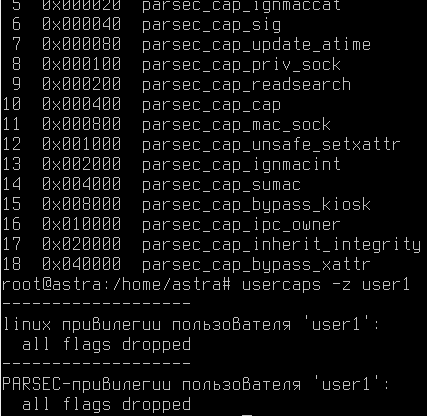


• с использованием графической утилиты «Политика безопасности» определить установленные привилегии и формат параметра модификации привилегий учётных записей пользователей (десятичная, восьмеричная или шестнадцатеричная система счисления при этом используется?);

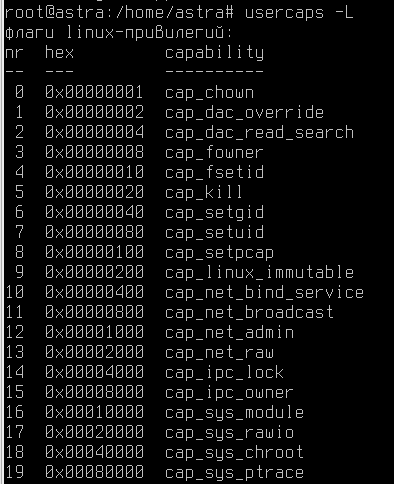
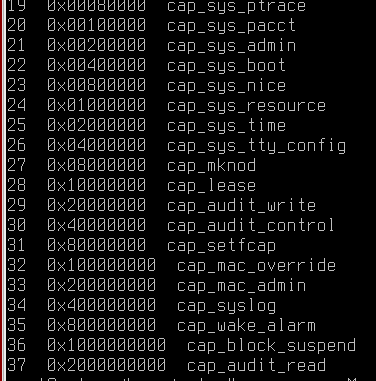


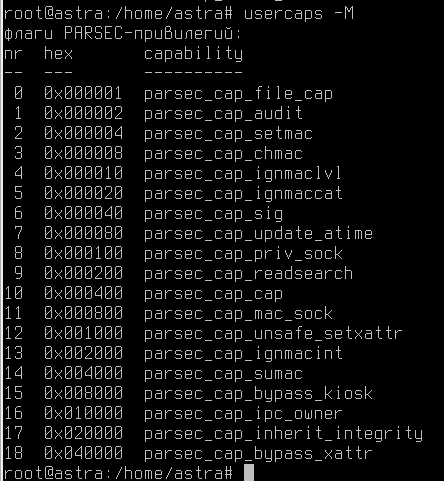
Используется 16-я система счисления.

• установить для учётной записи пользователя user1 полный список привилегий командой usercaps -f user1, затем удалить все привилегии учётной записи пользователя user1 командой usercaps -z user1;

• вывести списки Linux-привилегий и PARSЕС-привилегий командами usercaps -L и usercaps -М соответственно.



**Вывод:** в ходе лабораторной работы было изучено администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд.